UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,513	07/08/2003	R. Bruce Wallace	15929ROUS02U	9214

34645 7590 01/10/2008

JOHN C. GORECKI, ESQ.
P.O BOX 553
CARLISLE, MA 01741

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
01/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

john@gorecki.us

Office Action Summary	Application No.	Applicant(s)	
	10/615,513	WALLACE ET AL.	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2007(RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-11 and 13-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-11 and 13-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's submission for RCE filed on Oct. 25, 2007 has been entered. Claims 1-7, 9-11 and 13-25 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-3, 7, 9-11, 13-15 and 17, 18, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) and in view of Daniely (US Pub. No. 6,763,469).

As per claim 1, Hamilton teaches:

a local area network; one or more programmable logic controller [Fig. 1]; and a security policy implementation point (SPIP) connected between the network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the network [Fig. 1, 2, 6], the SPIP being configured participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network [Fig. 6, col. 9 lines 7-33].

Hamilton teaches the SPIP connected between the network and the one or more programmable logic controllers [Fig. 1, 6], which provides the authentication, authorization and/or other security measures when communicating activity data over a network [col. 9 lines 7-12, col. 10 lines 45-60].

Daniely teaches: a security policy implementation point (security device) connected between the local area network and the one or more component (device) to isolate the device from the local area network to prevent a person using a management program from accessing the one ore more devices over the local area network unless authenticated to the SPIP and authorized to take action on the SPIP, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel [Fig. 1A, 1B, col. 5 lines 1-10, 51-65, col. 6 lines 24-47].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Daniely with Hamilton, since one would have been motivated to provide flexible network security at the local level, which provides protection for computer/device against unauthorized access and permit authorized access within an organization [Daniely, col. 2 lines 42-44, col. 1 lines 60-63].

As per claim 2, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP, the programmable logic controller [Fig. 1, 6] and wherein the SPIP is logically connected between the network and the one or more programmable logic controllers [Fig. 1, 6].

Daniely teaches the SPIP (security policy/rules) is integrated with the programmable logic controllers (devices – e.g. computers, switches, routers, servers, gateways, devices) [Fig. 1A, 1B] and wherein the SPIP is logically connected between the local area network and the one or more devices/components [Fig. 1A].

As per claim 3, the rejection of claim 1 is incorporated and Hamilton teaches the network contains a plurality of programmable logic controller [Fig. 1], wherein the one or more programmable logic controller are subset of the plurality of programmable logic controllers [Fig. 1, 2] and wherein the SPIP is physically disposed between the network and the one or more programmable logic controllers [Fig. 1].

Daniely teaches the SPIP is physically connected between the local area network and the one or more devices/components [Fig. 1A].

As per claim 7, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is further configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the local area network through the SPIP to the one or more programmable logic controller [Fig.1, 6, col. 9 lines 7-33].

As per claim 9, the rejection of claim 1 is incorporated and Hamilton teaches the industrial network is an untrusted network configured to interconnect network services

with a plurality of SPIPs associated with factory machines, and wherein the network services are configured to enable operation of the factory machines to be altered through the industrial network [Fig. 1, 2, 6, col. 9 lines 7-33].

As per claim 10, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is further configured to enable local access to the one or more programmable logic controllers by applying a local authentication and authorization policy, to enable the SPIP to enforce network policy in connection with attempted local access [Fig. 1, 6, col. 9 lines 7-33].

As per claim 11, the rejection of claim 10 is incorporated and Hamilton teaches a local access policy configured to require authentication and authorization of at least one of an user and an. accessing electronic device for non-emergency attempts to access the SPIP, and an alternate access policy configured to allow access to the SPIP and maintain an audit log attendant to a local attempt to access the SPIP [Fig. 1, 6, col. 9 lines 7-33].

As per claim 13, the rejection of claim 11 is incorporated and Hamilton teaches the SPIP comprises a local authentication policy and information associated with authorized users and indicative of authorization policy information associated with said at least one factory machine [Fig. 1, 6, col. 9 lines 7-33].

Daniely teaches the local authentication policy and information associated with authorized users and devices [col. 5 lines 1-9, 50-63, col. 6 lines 24-41].

As per claim 14, Hamilton teaches:

a local path configured to implement a local access policy related to direct local access to one or more programmable logic controllers [Fig.1, 2, 6, col. 9 lines 7-33]; and a network path connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the industrial network [Fig. 1, 2, 6, col. 9 lines 7-33], the network path being configured to isolate the one or more programmable logic controllers and associated factory machines from the industrial network by participation in a Virtual Private Network such that communications with the SPIP over the industrial network utilize the Virtual Private Networks [Fig. 1, 2, 6, col. 9 lines 7-33].

Daniely teaches: a security policy implementation point (security device) connected between the local area network and the one or more component (device) to isolate the device from the local area network to prevent a person using a management program from accessing the one ore more devices over the local area network unless authenticated to the SPIP and authorized to take action on the SPIP, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel [Fig. 1A, 1B, col. 5 lines 1-10, 51-65, col. 6 lines 24-47].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Daniely with Hamilton, since one would have been motivated to provide flexible network security at the local level, which provides protection for computer/device against unauthorized access and permit authorized access within an organization [Daniely, col. 2 lines 42-44, col. 1 lines 60-63].

As per claim 15, the rejection of claim 14 is incorporated and Hamilton teaches programmable logic controller circuitry configured to implement the one or more programmable logic controllers and to function to control at least one factory machine [Fig. 1, 2].

As per claim 17, the rejection of claim 16 is incorporated and Hamilton teaches the local path further comprises an accounting module configured to record accesses to at least one of the SPIP, an associated programmable logic controller, and an associated factory machine [Fig. 1, 4, 5, 7].

As per claim 18, the rejection of claim 15 is incorporated and Hamilton teaches the local path comprises an authentication module configured to authenticate the identity of an individual seeking to access a device through the SPIP, and an authorization module configured to assess an authorization associated with the individual to ascertain whether the individual is authorized to access the device [Fig. 1, 6, col. 9 lines 7-33].

As per claim 21, the rejection of claim 15 is incorporated and Hamilton teaches the SPIP is configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the industrial network through the SPIP to the one or more programmable logic controllers [Fig. 1, 2, 6, col. 9 lines 7-33].

As per claim 22, the rejection of claim 15 is incorporated and Hamilton teaches network ports configured to interface with the industrial network, and output ports configured to interface with a programmable logic controller [Fig. 1, 2].

3. Claims 4-6 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) in view of Daniely (US Pub. No. 6,763,469) and in view of Danner et al (US Patent No. 7,194,003).

As per claim 4, the rejection of claim 3 is incorporated and Hamilton teaches the local area network is an Ethernet network, wherein the SPITP is configured to communicate with network devices on the local area network over the Ethernet network [Fig. 1, 2, col. 5 lines 55-60].

Danner teaches the switch is configured to communicate with the programmable logic controller using a protocol selected from at least one of Profibus, Controller Area Network, RS-232, RS-422, and RS-485 [col. 7 lines 1-9].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Danner with Hamilton and Daniely, since one would have been motivated to provide flexible network security at the local level [Daniely, col. 2 lines 43-44].

As per claim 5, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is included as blade in the network device [Fig. 6].

Danner teaches the local area network includes at least one Ethernet switch/router [Fig. 3].

As per claim 6, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is configured to implement security policy to control network access to at least one PLC through the SPIP [Fig. 1, 6, col. 9 lines 7-33]. Danner teaches at least one PLC connected to the Ethernet switch/router [Fig. 3].

As per claim 23, the rejection of claim 22 is incorporated and Hamilton teaches communication with the industrial control components and with remote devices as shown in Fig. 1, 2.

Danner teaches communicate on the industrial network utilizing an Ethernet protocol [col. 7 lines 17-39] and communicate with the programmable logic controller using a protocol understandable by the programmable logic controller [col. 7 lines 1-9].

As per claim 24, the rejection of claim 15 is incorporated and Danner teaches network ports configured to interface with the industrial network, control logic configured to implement a control program associated with a programmable logic controller, and interface ports configured to interface with a factory machine [Fig. 3, col. 6 lines 4-47].

As per claim 25, the rejection of claim 24 is incorporated and Danner teaches the interface ports comprise at least one input port configured to receive input from an environmental sensor, and at least one output port configured to control at least one electro-mechanical device [Fig. 3, col. 6 lines 4-47, 60-67, col. 7 lines 10-39].

4. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) in view of Daniely (US Pub. No. 6,763,469) and in view of Schmitz et al (US Patent No. 6,172,430).

As per claim 16, the rejection of claim 15 is incorporated and Hamilton teaches the local access policy for enabling access to the factory machine based on the authentication and authorization process associated with a user [col. 9 lines 7-24]. Hamilton doesn't

expressively mention to enable operation of the factory machine to be altered without verification of authorization and authentication of a user during an emergency.

Schmitz teaches: enable operation of the factory machine to be altered without verification of authorization and authentication of a user during an emergency [col. 5 lines 7-10].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Schmitz with Hamilton and Daniely, since one would have been motivated to prevent the hazardous condition.

5. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) in view of Daniely (US Pub. No. 6,763,469) and in view of Amara et al (US Pub. No. 2004/0083295).

As per claim 19, the rejection of claim 18 is incorporated and Hamilton teaches the authentication module and the authorization module [col. 9 lines 17-24].

Amara teaches interface to a Remote Access Dial In User Service (RADIUS) server [paragraph 0040]. Further, Amara teaches authentication and authorization mechanism utilize *other remote access software product* (e.g. RADIUS, DIAMETER, LDAP, etc.) [paragraph 0040, 0042].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Amara with Hamilton, since one would have been motivated to provide scalable network access system [Amara, paragraph 0006, 0007].

As per claim 20, the rejection of claim 18 is incorporated and Hamilton teaches the authentication and authorization modules maintain a local copy of authorized users and authentication policy to allow local access to the SPIP [col. 9 lines 24-29].

Amara teaches maintain a local copy of authorized users and authentication policy [paragraph 0046, 0047, 0027].

Response to Amendment

6. Applicant has amended claims 1 and 14, which necessitated new ground of rejection. See rejection above.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP
1/4/08